



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,271	02/20/2001	Gerhard Hoffmann	P00,1996	5299
21171	7590	12/15/2004	EXAMINER	
STAAS & HALSEY LLP SUITE 700 1201 NEW YORK AVENUE, N.W. WASHINGTON, DC 20005			POLTORAK, PIOTR	
			ART UNIT	PAPER NUMBER
			2134	

DATE MAILED: 12/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/763,271	Applicant(s) HOFFMANN ET AL.	
	Examiner Peter Poltorak	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 2/20/01.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date <u>2/20 and 7/12/01</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-20 have been examined.

Priority

2. Foreign priority has been claimed in this application.
3. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Germany on 08/18/1998.

Abstract

4. The abstract of the disclosure is objected to because the number "35" within the abstract body is not understood. Correction is required. See MPEP § 608.01(b).

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.
6. Claims 2, 4, 7-8, 12, 14 and 17-18 are rejected by virtue of their dependence.
7. Claim 1 recites, "forming a secret communication key ... which comprises a private key and a corresponding public key" then recites "said secret communication key and said public key forming an asymmetric cryptographic communication key pair". It is not clear whether "secret communication key" is the same as "private key". Public key cryptography involves two keys. One of them encrypts a message and

another one decrypts the message. It is not clear whether the invention attempts to introduce a "new system" in which three keys constitute the asymmetric cryptographic keys or whether the "private key" and the "secret key" are essentially the same key.

8. Similar ambiguity is observed in claim 10.
9. Similarly the difference between "said key pair" and "said communication key pair" in claims 3 and 13 is not understood.
10. The phrase "... to determine whether said checked number is a prime number and (determination of primacy)..." in claim 4 is not understood.
11. Claim 4 is not understood. One of the claim's limitations recites:

"selecting, when said number is not a prime number, another number based on said checked number and said index, said checked number being increased by a prescribed number".

"Said index" is addressed in another limitation as follows:

"said checked number is a prime, storing an index, which refers to a plurality of numbers, which have been checked with respect to their property of being prime"

It is unclear how the process is handled, especially for the first time when no number is checked with respect to their property of being prime, and as a result no index is created. Furthermore "selecting another number based on said checked number and said index" suggests that one would expect the selected number to be prime, and as a result the additional step "said checked number being increased by a prescribed number" is not understood.

Claim 14 presents similar problems.

12. "According to" the method of Miller-Rabin in claims 5 and 15 and "according to" the RSA method" in claims 6 and 16 are not clearly understood.

13. "Forming a digital signature via electronic data" in claims 9 and 19 is not understood.

14. Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

15. Claims 1-3, 6, 8 and 11-13, 16, 18 are rejected under 35 U.S.C. 102(b) as being anticipated by *Matyas et al.* (U.S. Patent No. 5201000).

16. As per claim 1, *Matyas et al.* teaches a method wherein users of a cryptographic device regenerate their secret keys by initially generating the public and private key pair from a passphrase provided to the key generation algorithm by the user (*col. 4 lines 58-66*). This reads on a prescribable initial value used in forming the secret communication key and the public key forming an asymmetric cryptographic communication key pair. Furthermore *Matyas et al.* teach Key Generation Using a Passphrase. In FIG. 13 *Matyas et al.* illustrate a cryptographic system comprising a cryptographic facility (CF) 30, a cryptographic key data set (CKDS) 32, a cryptographic facility access program (CFAP) 34, and application programs (APPL)

Art Unit: 2134

36. APPL A prompts the user for his/her passphrase (designated PP), which the user enters at 41. In response, APPL A calls KEY GENERATE function 47, at 43, located in the CFAP 34, passing a mode parameter, PP, and control information (designated control information) (*col. 18 lines 49-66*). This reads on the user entering the initial value into the computer.

17. As per claim 2, *Matyas et al.* teach *Key Generation Using a Passphrase*, wherein a user enters a passphrase. In response, the Key Generate function (47) parses the input to calculate a hash value (CW) from the input passphrase (*Fig. 13, col. 18 lines 49-11*). The hash value is passed to the key generation algorithm (KGA) which generates public and private keys (*Fig. 14 lines 28-36*). This reads on supplying the initial value to a hash function, and determining, using a hash function value formed by the hash function, the key pair and the communication key pair.

18. As per claim 3 additional data characterizing the user being utilized when the key pair and the communication key pair are being formed is inherent as *Matyas et al.* teach in col. 5 lines 16-17 that the system is shared by multiple users who use the device generating and purging their keys.

19. As per claim 6, *Matyas et al.* teach keys being formed according to the RSA method (*col. 12 lines 18-38*).

20. As per claim 8, secret communication keys inherently encipher data.

21. Claims 11-13, 16 and 18 are substantially equivalent to claims 1-3, 6 and 8; therefore claims 11-13, 16 and 18 are similarly rejected.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

22. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Matyas et al.* (U.S. Patent No. 5201000).

23. As per claim 4 *Matyas et al.* teach checking the initial value or a previously checked number (*checking a user input*), producing a checked number, to determine whether the checked number is a prime number (*Fig. 7*) and purging user's public and private keys (*col. 5 lines 22-23*) which reads on erasing a used prime number after the communication key pair has been formed. *Matyas et al.* also teach generating primes *Fig. 7* and suggests that the trial and error process of finding primes can be made more efficient by multiplying a checked number with a small number and then adding a number (*col. 14 lines 20-30*).

The act of multiplication is an abbreviated process of adding an integer to itself a specified number of times and an algorithm of adding numbers until the expected result is achieved (while loop, for example) are well known in the art. Therefore increasing the number that is not a prime number by a prescribed number would have been an obvious modification.

24. Claims 5 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Matyas et al.* (U.S. Patent No. 5201000) in view of *Menezes et al.* (Alfred J.

Menezes, Paul C. van Oorschot, Scott A. Vanstone, "Handbook of applied cryptography", 1997, ISBN: 0849385237).

Matyas et al. teach the determination of primacy for any given number as discussed above.

Matyas et al. do not teach the determination of primacy for any given number carried out according to the method of Miller-Rabin.

Menezes et al. teach determination of primacy for any given number carried out according to the method of Miller-Rabin (*Menezes et al.*, pg. 138-140).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use determination of primacy for any given number carried out according to the method of Miller-Rabin as taught by *Menezes et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to make sure that the numbers identified as prime were always correct (*Menezes et al.* pg. 140, § 6).

25. Claims 7 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Matyas et al.* (U.S. Patent No. 5201000).

Matyas et al. teach a hash function as discussed above.

Matyas et al. do not explicitly teach using the MD-5, MD-2 or DES.

However, the choice of MD-5, MD-2 or DES as a hash function would have been obvious to one of ordinary skill in the art given that they are well known and barring any unexpected results.

26. Claims 9-10 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Matyas et al.* (U.S. Patent No. 5201000) in view of Official Notice.

27. *Matyas et al.* teach a secret key generation as discussed above and teach the network providing the means for sending and receiving encrypted data (col. 2 lines 65-67).

Matyas et al. do not explicitly teach forming a digital signature via electronic data using the secret communication key nor does he teach the step authenticating data using said secret communication key.

Official Notice is taken that it is old and well-known in the art to use a secret communication key to form a digital signature and a digital signature to provide data authentication. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to form a digital signature via electronic data using the secret communication key and to provide data authentication using the digital signature.

One of ordinary skill in the art would have been motivated to perform such a modification in order to provide non-repudiation.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

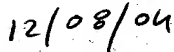
Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Signature



Date



GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100